US 20120158574A1

(19) **United States**

(12) **Patent Application Publication**

Brunzell et al.

(10) **Pub. No.: US 2012/0158574 A1**

(43) **Pub. Date: Jun. 21, 2012**

(54) **SYSTEMS AND METHODS FOR DETECTING BUST OUT FRAUD USING CREDIT DATA**

(75) Inventors: **Hakan Olof Brunzell**, Costa Mesa, CA (US); **Arielle Renee Caron**, Irvine, CA (US); **Tak Wun Wong**, Culver City, CA (US); **Anthony J. Sumner**, Nottingham (GB)

(73) Assignee: **Experian Information Solutions, Inc.**, Costa Mesa, CA (US)

(21) Appl. No.: **13/186,130**

(22) Filed: **Jul. 19, 2011**

Related U.S. Application Data

(63) Continuation of application No. 12/904,088, filed on Oct. 13, 2010, now Pat. No. 8,001,042, which is a continuation of application No. 12/220,320, filed on Jul. 23, 2008, now Pat. No. 7,991,689.

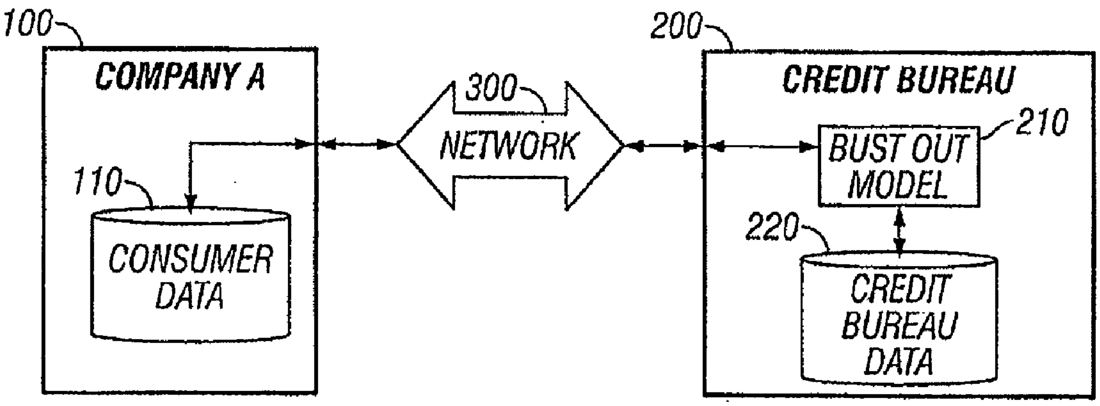
Publication Classification

(51) **Int. Cl.**
G06Q 40/02 (2012.01)

(52) **U.S. Cl.** **705/38**

(57) **ABSTRACT**

Systems and methods are disclosed for predicting bust out fraud using credit bureau data. In one embodiment, credit bureau scoring models are created using credit bureau data to detect bust out fraud. The credit bureau scoring models may be then applied to consumer data to determine whether a consumer is involved in bust out fraud.



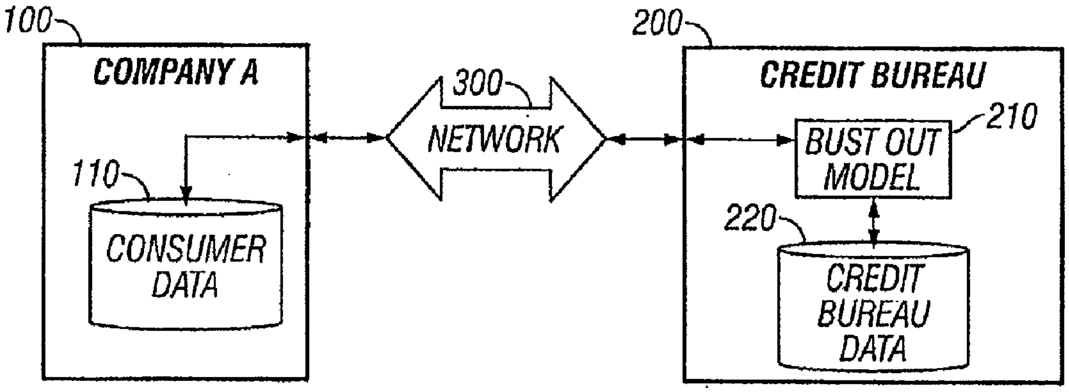

100
COMPANY A
110
CONSUMER DATA
300
NETWORK
200
CREDIT BUREAU
BUST OUT MODEL
210
220
CREDIT BUREAU DATA

FIG. 1

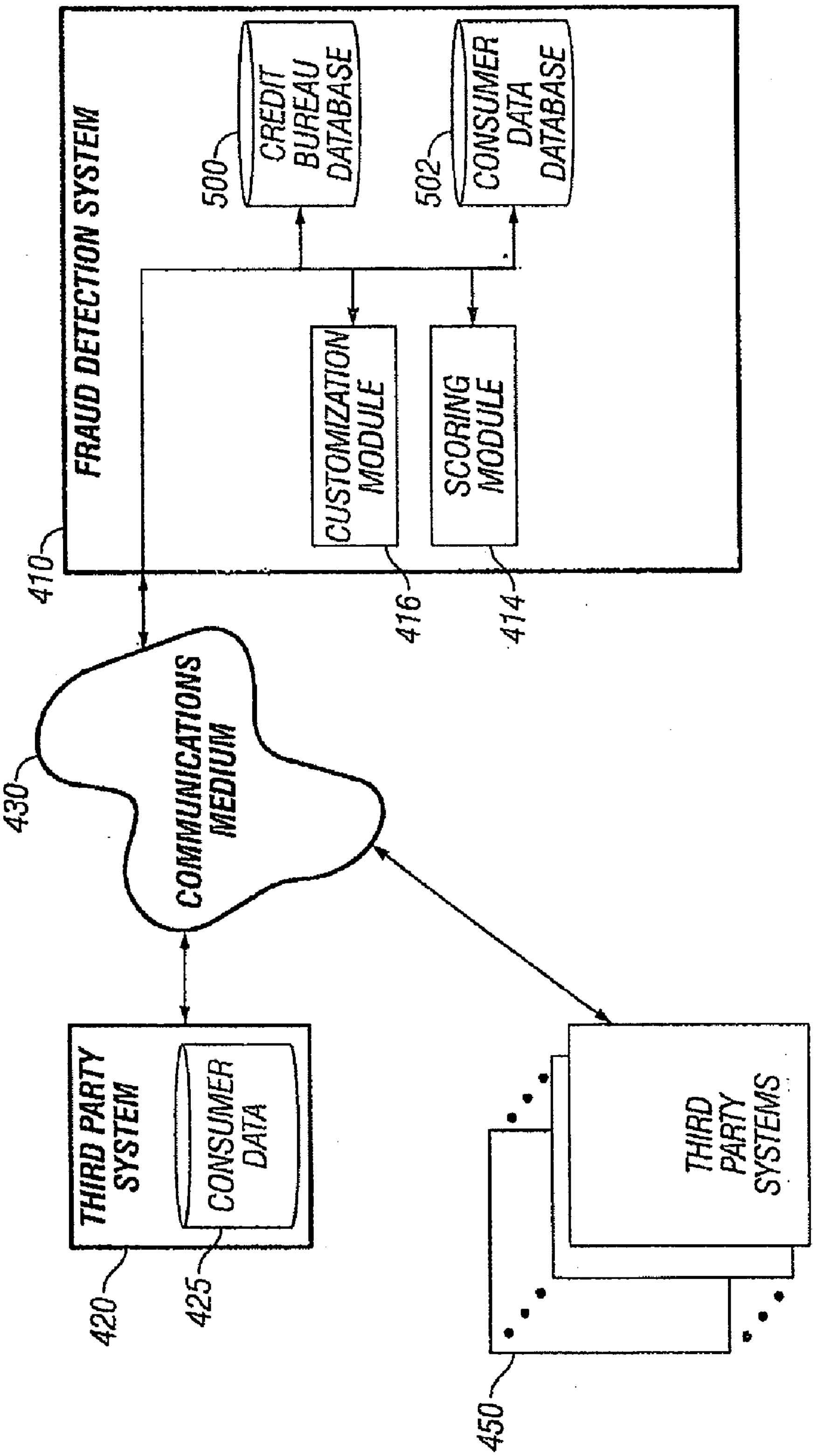

FRAUD DETECTION SYSTEM
410
500
CREDIT BUREAU DATABASE
502
CONSUMER DATA DATABASE
CUSTOMIZATION MODULE
416
SCORING MODULE
414
COMMUNICATIONS MEDIUM
430
THIRD PARTY SYSTEM
420
CONSUMER DATA
425
THIRD PARTY SYSTEMS
450

FIG. 2

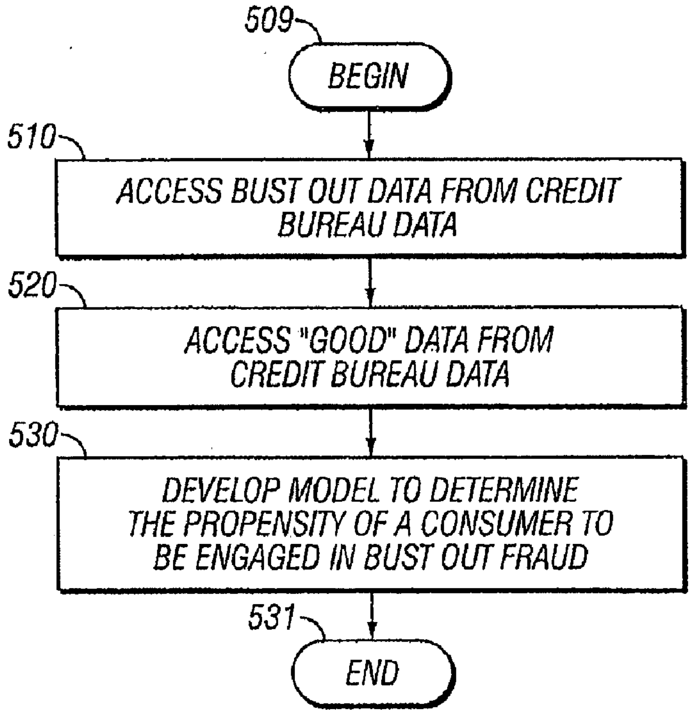

509
BEGIN
510
ACCESS BUST OUT DATA FROM CREDIT BUREAU DATA
520
ACCESS "GOOD" DATA FROM CREDIT BUREAU DATA
530
DEVELOP MODEL TO DETERMINE THE PROPENSITY OF A CONSUMER TO BE ENGAGED IN BUST OUT FRAUD
531
END

FIG. 3

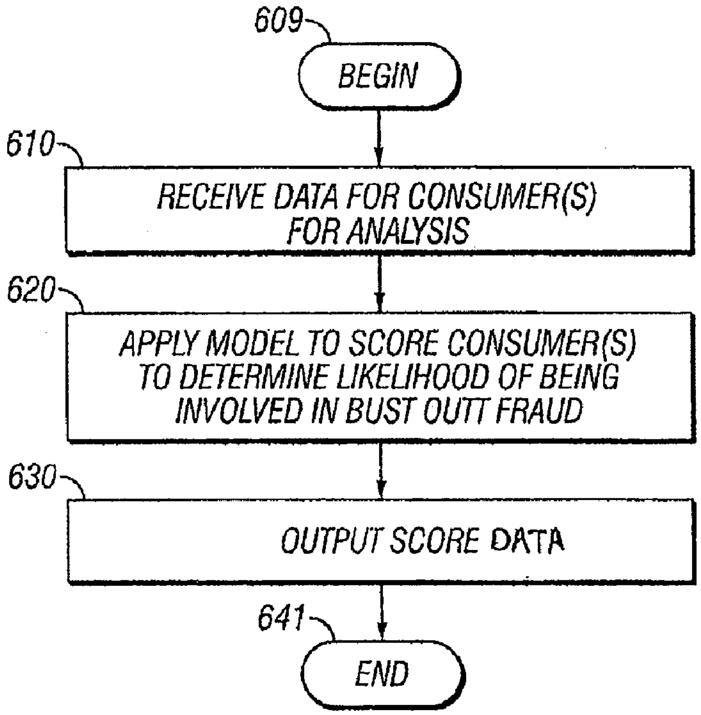

609
BEGIN
610
RECEIVE DATA FOR CONSUMER(S) FOR ANALYSIS
620
APPLY MODEL TO SCORE CONSUMER(S) TO DETERMINE LIKELIHOOD OF BEING INVOLVED IN BUST OUTT FRAUD
630
OUTPUT SCORE DATA
641
END

FIG. 4

SYSTEMS AND METHODS FOR DETECTING BUST OUT FRAUD USING CREDIT DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation of U.S. patent application Ser. No. 12/904,088, filed Oct. 13, 2010, entitled SYSTEMS AND METHODS FOR DETECTING BUST OUT FRAUD USING CREDIT DATA, which is a continuation of U.S. patent application Ser. No. 12/220,320, filed Jul. 23, 2008, now U.S. Pat. No. 7,991,689. The foregoing applications and patent are hereby incorporated herein by reference in their entirety, including specifically but not limited to the systems and methods relating to bust out fraud detection.

BACKGROUND

[0002] 1. Field of the Invention

[0003] The disclosure relates generally to the field of financial protection. The disclosure relates specifically to the field of fraud detection.

[0004] 2. Description of the Related Art

[0005] The occurrence of fraud and related dollar losses is growing because it has been very difficult for the financial industry to detect bust out fraud using traditional fraud detection systems. Traditional fraud detection systems are typically applied in two ways: at the point of credit application (sometimes referred to as application fraud systems), or through ongoing monitoring by a financial institute of its consumer transactions compared against an established profile of that consumer's behavior (sometimes referred to as transaction fraud systems).

[0006] Application fraud systems were not designed to detect fraud that takes place after the consumer's application is approved and credit is granted (sometimes referred to as post-book fraud); consequently, such systems often prove ineffective in detecting post-book fraud. For example, if a consumer is opening an account in his/her own name intending to commit fraud in the future, application fraud systems may verify the consumer's identity without analyzing the likelihood of the consumer engaging in fraud after the account is opened. Similarly, transaction fraud systems are ineffective in situations when evolving types of fraud that take advantage of more than one financial institution.

SUMMARY OF THE DISCLOSURE

[0007] One specific type of fraud that traditional fraud systems are unable to detect is fraud that typically occurs in an organized fashion, across multiple credit issuers, and involves a build-up phase of seemingly normal consumer behavior followed by an exceedingly large number of purchases, cash advances, or other uses of credit, and then subsequent abandonment of the account. This fraud is sometimes referred to as bust out fraud.

[0008] Consequently, it would be advantageous to have methods and systems that automatically detect such fraudulent activity. In some embodiments, credit bureau scoring models are created using credit bureau data to detect bust out fraud. The credit bureau scoring models may be then applied to consumer data to determine whether a consumer is likely involved in bust out fraud before a consumer abandons his accounts.

[0009] In one embodiment, a computer implemented method of developing a data filter for identifying bust out fraud is disclosed. The computer implemented method may include electronically developing a credit bureau bust out model that predicts the propensity of a consumer to be engaged in bust out fraud analyzing substantially only credit bureau data.

[0010] In another embodiment, a bust out fraud detection system is disclosed. The bust out fraud system may include a processor configured to run software modules; a data storage device storing a plurality of consumer records, the data storage device in electronic communication with the processor; and a bust out module configured to identify a subset of the plurality of records from the data storage device, receive a credit bureau bust out model from a storage repository, the credit bureau bust out model predicting which consumer records are likely involved and created using substantially only credit bureau data, apply the credit bureau bust out model to each of the subset of the plurality of consumer records to generate a credit bureau bust out score for each of the subset of the plurality of consumer records, and store in a storage repository the credit bureau bust out score associated with the subset of the plurality of the consumer records; and where the processor is able to run the bust out module.

[0011] In a further embodiment, a computer implemented method for generating scores that indicate bust out fraud is provided. The computer implemented method may include electronically identifying a plurality of consumer records; electronically receiving a bust out filter from a storage repository, the bust out filter created using substantially only credit bureau data; electronically applying the bust out filter to each of the plurality consumer records to generate a bust out score for each of the plurality of consumer records; and electronically storing in a storage repository the bust out score associated with each of the consumer records.

[0012] For purposes of the summary, certain aspects, advantages and novel features of the invention have been described herein. Of course, it is to be understood that not necessarily all such aspects, advantages or features will be embodied in any particular embodiment of the invention. Thus, for example, those skilled in the art will recognize that the invention may be embodied or carried out in a manner that achieves one advantage or group of advantages as taught herein without necessarily achieving other advantages as may be taught or suggested herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The foregoing and other features, aspects and advantages of the present invention are described in detail below with reference to the drawings of various embodiments, which are intended to illustrate and not to limit the invention. The drawings comprise the following figures.

[0014] FIG. **1** illustrates one embodiment of example scenario for detecting bust out fraud using credit bureau data.

[0015] FIG. **2** illustrates one embodiment of a computer hardware system configured to run software for implementing one or more embodiments of the fraud detection system described herein.

[0016] FIG. **3** illustrates one embodiment of a flowchart diagram for analyzing data to create a credit bureau bust out model using credit bureau data.

[0017] FIG. **4** illustrates one embodiment of a flowchart diagram for analyzing consumer data to apply a credit bureau bust out model and generate credit bureau bust out scores.

DETAILED DESCRIPTION

[0018] Embodiments of the invention will now be described with reference to the accompanying figures, wherein like numerals refer to like elements throughout. The terminology used in the description presented herein is not intended to be interpreted in any limited or restrictive manner, simply because it is being utilized in conjunction with a detailed description of certain specific embodiments of the invention. Furthermore, embodiments of the invention may comprise several novel features, no single one of which is solely responsible for its desirable attributes or which is essential to practicing the inventions herein described. In addition, it is recognized that a feature of one embodiment may be included as a feature in a different embodiment.

[0019] Some embodiments discussed herein provide systems and methods for predicting bust out fraud. "Bust out" fraud is a hybrid fraud and credit problem were an individual and/or entity opens multiple lines of credit/accounts increases utilization and then subsequently abandons the accounts. The line of credit/accounts may include credit cards accounts, debit card accounts, equity lines, and so forth. In one embodiment, scoring models are specifically developed to predict bust out fraud using credit bureau data. One advantage to using credit bureau data is that it provides information about the consumer across multiple consumer accounts at multiple institutions. The scoring models can be applied to one or more sets of consumer data to generate a score for each consumer predicting the likelihood that the consumer is involved in bust out fraud. The scoring models can then be used alone or in combination with other scores and credit or demographic attributes to evaluate a consumer when opening an account, to monitor a portfolio of consumers, and/or to weed out undesirable prospective customers. In addition, the scoring model may be used in an online environment or in a batch environment.

[0020] In one embodiment, the scoring model is created using "bad" credit bureau data, which includes data for accounts that were classified as bust out accounts. In some embodiments, an account is classified as a bust out fraud account according to two aspects, action and intent. Example account actions include, an account balance approaching or exceeding its limit, payments with bad checks, and/or similar behavior on other accounts linked to the same account holder. Example account actions demonstrating intent include requests for a credit limit increase, requests for adding authorized users, frequent balance inquiries, use of balance transfers and convenience checks, and/or being unable to contact the account holder. In other embodiments, other requirements or definitions may be used to classify an account or a consumer as a bust out account. Thus, the bad credit bureau data used to create the scoring module may include a variety of data including, for example, data indicating that an account is unpaid, the account is delinquent (for example 30^+ days, 60^+ days, 90^+ days, 120^+ days), the accounts balance is close to or over its limit, a payment on the account has been returned or bounced, attempts to contact the account owner via the providers phone number(s), address(es), and/or email address (es) have failed, and/or that similar data exists at one or more financial institutions. The scoring model may also be created using "good" credit bureau data, which is data from non-fraud consumers.

[0021] The scoring models may be configured in a variety of ways. For example, the scoring models may be configured to enhance the prediction of bust out fraud, to reflect current bust out fraud trends, to increase the operational efficiency of identifying consumers that may be involved in bust out fraud, and/or to compliment existing fraud detection/prevention tools. The scoring models also may be configured to predict bust out fraud for a certain amount of time prior to the abandoning of any accounts, such as, for example 6 to 8 weeks, or 1 to 3 months. In addition, the scoring models may be configured to detect a significant portion of bust out fraud such as, for example 35%, 60%, or 78% of bust out fraud. The scoring models also may be configured designate high risk consumers (for example, consumers with a higher score) from low risk consumers (for example, consumers with a lower score) so that the user of the system can focus on dealing with the higher risk consumers. The scoring model may also factor in the potential amount at risk such that consumers that are most likely involved in bust out fraud and that have the highest potential collection balance are scored the highest.

[0022] The scoring models may utilize a variety of scoring methods, including numeric scores where the lower number indicates bust out fraud, numeric scores where a higher number indicates bust out fraud, letters scores (for example A, B, C, D or F), categories (for example good, bad), and so forth.

[0023] Moreover, the scoring models may be configured to incorporate information on consumers that are flagged as potential "bust outs," but do not end up as "bust outs." The system may use the flagging of such "false positives" to look for other potentially harmful activity and/or further refine the scoring model.

[0024] In some embodiments, the fraud detection system may advantageously be used alone or in combination with other scoring models and credit or demographic attributes to analyze a portfolio of consumers or prospective consumers. In some embodiments, these scores and/or attributes may be used with customizable thresholds (for example, tolerance levels for an amount of change). For example, one scoring model may evaluate changes in utilization, such as a consumer's use of credit against maximum available credit, and detect unusual velocity such as the number of new accounts opened or inquiries received in a certain time frame. Attributes may include changes in demographic information, such as a change in address or phone number. One scoring model may detect a pattern of suspicious payment behaviors, such as nonpayment, delinquency, returned payment, smaller-than-usual payments, or larger-than-usual payments. Other elements of the scoring model may include cross-database entity matching and pattern analysis to detect organized and/or collusive behaviors. It is recognized that many other attributes, scores, and/or model elements that may be used.

[0025] In general, the term "model" as used herein is a broad term, and generally refers without limitation to systems, devices, and methods for amplifying, selecting, filtering, excluding, predicting, and/or identifying subsets of a dataset that are relevant, substantially relevant, and/or statistically relevant to the user. In addition, the terms "consumer" and "consumers" may include applicants, customers, individuals, entities, groups of individuals, (for example, married couples, domestic partners, families, co-workers, and the likes), and so forth. Furthermore, the terms "financial entity," "credit providers," "credit issuers," "financial institutions," "clients," "utility providers," "utility service providers," "phone service providers," "financial service providers," are broad interchangeable terms and generally refer without limitation to banks, financial companies, credit unions, savings institutions, retailers, utility (for example, telecommunications, gas, electric, water, sewer, or the like) providers, bankcard issuers, credit card issuers, mortgage (for example, subprime) lenders, and the like.

I. Example Scenario

[0026] One example scenario will now be discussed with respect to FIG. **1**, which shows a sample embodiment for using a scoring model that predicts bust out fraud using credit bureau data.

[0027] In the example, Company A **100** is a department store that provides credit cards for a large number of consumers. However, Company A **100** has been having problems with bust out accounts where several of its consumers have built up their credit, reached a maximum credit line on their accounts, and then abandoned their accounts. Thus, Company A **100** wants to know before consumers abandon their accounts, whether a particular consumer is engaging in bust out fraud. Company A's **100** own consumer data does not provide a full picture of a consumer since the bust out behavior may be the result of a consumer's activity at other companies, such as Company B and/or Company C. Accordingly, Company decides to contact Credit Bureau **200** for assistance.

[0028] The Credit Bureau **200** stores data **220** about consumers, and part of that data includes consumer credit activities, balance, available credit and utilization, depth of credit experience, delinquency and derogatory statuses on tradelines, both current and historical, derogatory public records and inquiry history. The Credit Bureau **200** decides to use this data **220** to create a bust out model **210** that scores consumer data indicating whether a consumer is engaged in bust out fraud. To create the bust out model **210**, the Credit Bureau **200** collects bad and good data from its credit bureau data **220**, analyzes the data, and creates a bust out model **210** that predicts which consumers may be involved in bust out fraud.

[0029] Company A **100** then sends the Credit Bureau **200** a set of its consumer data for Company A's **100** existing customers over the network **300**. The Credit Bureau **200** applies the bust out model **210** in batch mode to Company A's **100** set of consumer data to determine which consumers may be involved in bust out fraud and creates a set of bust out score data. This bust out score data includes bust out scores along with consumer identifiers for each score. The Credit Bureau **200** then sends the bust out score data back to Company A **100** over the network **300**, and Company A uses the scores to flag existing consumers for immediate investigation.

[0030] Company A **100** may also send the Credit Bureau **200** a set of consumer data for its prospective consumers, which are consumers Company A **100** would like to send an offer of credit. The Credit Bureau **200** applies the bust out model **210** in batch mode to Company A's **100** set of consumer data to determine which consumers may be involved in bust out fraud and creates a set of bust out scores. For this data, Company A **100** has requested that the Credit Bureau **200** append the scores to the set of consumer data. Thus, Credit Bureau **200** then sends the set of consumer data, which now includes the scores, back to Company A **100**. Company A **100** uses the scores to remove some of the consumers from the set of prospective consumers since Company A **100** does not want to extend an offer of credit to a consumer who has a high likelihood to be engaged in bust out fraud.

[0031] Next, as part of its credit application process, Company A **100** sends the Credit Bureau **200** a set of consumer data for new customers that are applying at the store for credit from Company A **100**. The Credit Bureau **200** then applies the bust out model **210** to the set of consumer data and sends bust out score data, which includes a score for each consumer in the set of consumer data, back to Company A. Company A then uses the scores to decide whether to approve or deny the credit applications for each of the consumers.

[0032] FIG. **1** and the example scenario above, provide an embodiment of using the systems and methods disclosed here, and are not intended to be limiting in any way.

II. Data

[0033] A. Credit Bureau Data

[0034] The scoring models are created using samples of credit bureau data using both bad data (for example, bust out account data) and good data (for example, non-fraud account data). In one embodiment, the samples of credit bureau data include a minimum number of bad accounts, such as, for example, 100 bust out accounts, 1000 bust out accounts, 3128 bust out accounts, or 5000 bust out accounts, though the number of bad accounts included may vary. The sample of credit bureau data may also include a random sampling of non-fraud accounts or a selected sampling of non-fraud accounts. In one embodiment, non-fraud data includes credit bureau data for accounts that are not involved in bust out fraud, whereas in other embodiments, non-fraud data includes credit bureau data for accounts that are not involved in any type of fraud. In one embodiment, the number of non-fraud accounts is approximately 20 to 13000 times the number of bad accounts.

[0035] B. Consumer Data

[0036] In some embodiments, some or all of the consumer data to be scored is received from a third party. The consumer data may include data for one or more consumers and may be received in real-time or in batch format. In one embodiment, the third party sends the data in an encrypted format, such as, for example PGP encryption, password protection using WinZip 9.1 or higher with 256-Bit encryption, or any other encryption scheme. In addition, the consumer data may be sent via a secure connection, an email, File Transmission Protocol site, ConnectDirect Mailbox, a disk, tape drive, zip drive, CD-ROM, and so forth.

[0037] In one embodiment, the third party providing the consumer data is the same party that is receiving the bust out score data. It is recognized that in other embodiments, a different party may receive the bust out score data than the one that submits the consumer data, and/or multiple parties may provide consumer data and/or multiple parties may receive the bust out score data.

[0038] C. Bust Out Score Data

[0039] In one embodiment, the bust out score data includes the scores generated by the scoring model along with corresponding identifiers for the consumers in the set of consumers data. The bust out score data may also include reason code data that indicates factors that contributed to one or more of the scores. The bust out score data may include data for one or more consumer and may be sent in real-time or in batch format. In other embodiments, the bust out score data only includes scores, includes other consumer data, and or is appended to the consumer data.

[0040] In one embodiment, the bust out score data is sent to a third party in an encrypted format, such as, for example PGP encryption, password protection using WinZip 9.1 or higher with 256-Bit encryption, or any other encryption scheme. In addition, the bust out score data may be sent via a secure connection, an email, File Transmission Protocol site, ConnectDirect Mailbox, a disk, tape drive, zip drive, CD-ROM, and so forth.

III. Fraud Detection System

[0041] FIG. **2** illustrates one embodiment of a fraud detection system **410** that creates scoring models using credit bureau data, where the scoring models predict whether a consumer will engage in bust out fraud. The fraud detection system **410** also applies the created scoring models to predict whether a particular consumer or set of consumers are engaging in bust out fraud and scores the consumer or set of consumers to indicate whether they are likely involved in bust out fraud. The exemplary fraud detection system **410** communicates with a third party system **420** via a communications medium **430** and includes a scoring module **414** for creating a scoring model using credit bureau data and scoring consumers in a data file along with a customization module **416** that allows the third party system **420** to set preferences, thresholds and/or tolerance levels for defining "bust out" data, creating the scoring model, applying the scoring model, formatting the bust out score data, and setting up the data exchange. The fraud detection system **410** also includes a processor (not shown) configured to run modules, such as **414** and **416**. The fraud detection system **410** also includes a credit bureau database **500** that stores credit bureau data, such as, for example, consumer data, account data, non-fraud account data, and/or bad account data.

[0042] In one embodiment, the fraud detection system retrieves credit bureau data from the credit bureau database **500** and uses that data to create a scoring model. The fraud detection system **410** then receives third party system **420** consumer data **425** and applies the scoring model to the third party system **420** consumer data **425**. In other embodiments, the fraud detection system **410** can also apply the scoring model to consumer data **455** from other third party systems **450**. The fraud detection system **410** may also include a consumer data database **502** that stores all or a subset of the third party consumer data **425** as well as some or all of the bust out score data. For example, the consumer data database **502** may store consumer identity information and a history information regarding one or more of the provided scores. It some embodiments, the fraud detection system **410** may also communicate with other systems (not shown).

IV. System Information

[0043] A. Computing Devices

[0044] In one embodiment, the fraud detection system **410** and/or the third party systems **420**, **450** run on one or more computing devices. Moreover, in some embodiments, the features of the fraud detection system **410** and/or the third party systems **420**, **450** may be available via a fully-hosted application service provider (ASP) that manages and provides communication between the fraud detection system **410** and one or more of the third party systems **420**, **450** via a web interface or other interface. In other embodiments, the fraud detection system **410** and/or the third party systems **420**, **450** may be available via partially-hosted ASPs or other providers. In yet further embodiments, the fraud detection system **410** and/or the third party systems **420**, **450** may be a client-side installed solution allowing for direct communication between the fraud detection system **410** and one or more of the third party systems **420**, **450**.

[0045] In one embodiment, the computing device is IBM, Macintosh, or Linux/Unix compatible devices. In another embodiment, the computing device comprises a server, a laptop computer, a cell phone, a personal digital assistant, a kiosk, or an audio player, for example. In one embodiment, the computing device includes one or more CPUs, which may each include microprocessors. The computing device may further include one or more memory devices, such as random access memory (RAM) for temporary storage of information and read only memory (ROM) for permanent storage of information, and one or more mass storage devices, such as hard drives, diskettes, or optical media storage devices.

[0046] In one embodiment, the modules of the computing are in communication via a standards based bus system, such as bus systems using Peripheral Component Interconnect (PCI), Microchannel, SCSI, Industrial Standard Architecture (ISA) and Extended ISA (EISA) architectures, for example. In some embodiments, components of the computing device communicate via a network, such as a local area network that may be secured.

[0047] The computing device is generally controlled and coordinated by operating system software, such as the Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista, Linux, SunOS, Solaris, PalmOS, Blackberry OS, or other compatible operating systems. In Macintosh systems, the operating system may be any available operating system, such as MAC OS X. In other embodiments, the computing device may be controlled by a proprietary operating system. Conventional operating systems control and schedule computer processes for execution, perform memory management, provide file system, networking, and I/O services, and provide a user interface, such as a graphical user interface (GUI), among other things.

[0048] The computing device may include one or more commonly available input/output (I/O) devices and interfaces, such as a keyboard, mouse, touchpad, microphone, and printer. Thus, in one embodiment the computing device may be controlled using the keyboard and mouse input devices, while in another embodiment the user may provide voice commands to the computing device via a microphone. In one embodiment, the I/O devices and interfaces include one or more display device, such as a monitor, that allows the visual presentation of data to a user. More particularly, a display device provides for the presentation of GUIs, application software data, and multimedia presentations, for example. The computing device may also include one or more multimedia devices, such as speakers, video cards, graphics accelerators, and microphones, for example.

[0049] In one embodiment, the computing devices include a communication interface to various external devices and the communications medium **430** via wired or wireless communication links.

[0050] B. Data Sources

[0051] The data sources, including the consumer data **425**, the credit bureau database **500**, and the consumer data database **502**, may include one or more internal and/or external data sources. In some embodiments, one or more of the data sources may be implemented using a relational database, such as, for example, Sybase, Oracle, CodeBase and Microsoft® SQL Server as well as other types of databases such as, for example, a flat file database, an entity-relationship database, and object-oriented database, and/or a record-based database.

[0052] C. Modules

[0053] In general, the word "module," as used herein, refers to logic embodied in hardware or firmware, or to a collection of software instructions, possibly having entry and exit points, written in a programming language, such as, for example, Java, C or C++. The module may include, by way of example, components, such as, for example, software components, object-oriented software components, class components and task components, processes, functions, attributes, procedures, subroutines, segments of program code, drivers, firmware, microcode, circuitry, data, databases, data structures, tables, arrays, and variables. A software module may be compiled and linked into an executable program, installed in a dynamic link library, or may be written in an interpreted programming language such as, for example, BASIC, Perl, or Python. It will be appreciated that software modules may be callable from other modules or from themselves, and/or may be invoked in response to detected events or interrupts. Software instructions may be embedded in firmware, such as an EPROM. It will be further appreciated that hardware modules may be comprised of connected logic units, such as gates and flip-flops, and/or may be comprised of programmable units, such as programmable gate arrays or processors. The modules described herein are preferably implemented as software modules, but may be represented in hardware or firmware. Generally, the modules described herein refer to logical modules that may be combined with other modules or divided into sub-modules despite their physical organization or storage.

[0054] D. Communications Medium

[0055] In the embodiment of FIG. **2**, the communications medium **430** is one or more networks, such as, for example, a LAN, WAN, or the Internet, for example, via a wired, wireless, or combination of wired and wireless, communication link. The communications medium **430** communicates with various computing devices and/or other electronic devices via wired or wireless communication links. For example, the computing device may be configured to communicate with the communications medium using any combination of one or more networks, LANs, WANs, or the Internet, for example, via a wired, wireless, or combination of wired and wireless communication links. It is also recognized that one or more the third party systems **420**, **450** and the fraud detection system **410** may communicate using two or more different types of communications mediums **430**, and the fraud detection system **410** may communicate with one or more of the third party systems **420**, **450** using different types of communications mediums **430**.

V. Flowcharts

[0056] A. Creating Bust Out Models Using Credit Data

[0057] FIG. **3** illustrates an embodiment of a flowchart showing one method (for example, a computer implemented method) of analyzing credit bureau data (for example, bad data and good data) to create bust out models. The method can be performed online, in real-time, batch, periodically, and/or on a delayed basis for individual records or a plurality of records. The exemplary method may be stored as a process accessible by the scoring module **414** and/or other modules of the fraud protection system **410**. In different embodiments, the blocks described below may be removed, others may be added, and the sequence of the blocks may be altered.

[0058] With reference to FIG. **3**, the method is initiated (block **509**), and the fraud detection system **410** accesses bust out credit bureau data (block **510**). The fraud detection system **410** also accesses non-fraud credit bureau data (block **520**). In an embodiment, the bust out credit bureau data and non-fraud credit bureau data include consumer demographic, credit, and other credit bureau data (for example, historical balance data for a period of time, credit limits data for a period of time, or the like). Specific criteria for being categorized as a bust out data may vary greatly and may be based on a variety of possible data types and different ways of weighing the data. The bust out and/or non-fraud credit bureau data may also include archived data or a random selection of credit bureau data.

[0059] The fraud detection system **410** develops a model using the bust out credit bureau data and the non-fraud credit bureau data (block **530**), which determines whether a consumer is involved in bust out fraud. In one embodiment, the development of the model comprises identifying consumer characteristics, attributes, or segmentations that are statistically correlated (for example, a statistically significant correlation) with the occurrence of a bust out account. The development of the model may include developing a set of heuristic rules, filters, and/or electronic data screens to determine and/or identify and/or predict which consumer profiles would be classified as a bust out account based on the credit bureau data. The development of the model can also include developing a set of heuristic rules, filters, and/or electronic data screens to determine and/or identify and/or predict which data is attributable to bust out accounts based on the credit bureau data.

[0060] It is recognized that other embodiments of FIG. **3** may be used. For example, the method of FIG. **3** could be repeatedly performed to create multiple bust out models, the non-fraud credit bureau data may be accessed before the bust out credit bureau data, and/or the bust out credit bureau data and the non-fraud credit bureau data may be accessed at the same time or in parallel.

[0061] B. Using The Bust Out Models To Score Consumer Data

[0062] FIG. **4** illustrates an embodiment of a flowchart illustrating a method of applying a bust out model, which was created using credit data, to predict whether a consumer to be involved in bust out fraud. The exemplary method may be stored as a process accessible by the scoring module **414** and/or other components of the fraud detection system **410**. In some embodiments, the blocks described below may be removed, others may be added, and the sequence of the blocks may be altered.

[0063] With reference to FIG. **4**, the method is initiated (block **609**), and the fraud detection system **410** selects or receives consumer data (block **610**). The consumer data includes data for one or more consumers. In some embodiments, the fraud detection system **410** may also obtain consumer data from a third party system **420**, **450** and/or the consumer data database **502**. The fraud detection system **410** analyzes the consumer data by applying the bust out model to the data, generates generate a score(s) indicating the likelihood that the consumer(s) is involved in bust out fraud (block **620**). The fraud detection system **410** then outputs bust out score data (block **630**). The bust out score data may be sent to a third party system **420**, the user, another module, another system, and/or stored in the consumer data database **502**, or the like.

[0064] It is recognized that other embodiments of FIG. **4** may be used. For example, the method of FIG. **4** could stored the bust out score data in a database and/or apply additional rules such as, for example, removing data for consumers that are not involved in bust out fraud.

VI. Additional Embodiments

[0065] Although the foregoing has been described in terms of some embodiments, other embodiments will be apparent to those of ordinary skill in the art from the disclosure herein. Moreover, the described embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions. Indeed, the novel methods and systems described herein may be embodied in a variety of other forms without departing from the spirit thereof. Accordingly, other combinations, omissions, substitutions, and modifications will be apparent to the skilled artisan in view of the disclosure herein.

What is claimed is:

1. A bust out fraud detection system, the system comprising:

a processor configured to run software modules;

a data storage device storing a plurality of consumer records, the data storage device in electronic communication with the processor; and

a bust out module configured to:

identify a subset of the plurality of records from the data storage device;

receive a credit bureau bust out model from a storage repository, the credit bureau bust out model predicting which consumer records are likely involved and created using substantially only credit bureau data;

apply the credit bureau bust out model to each of the subset of the plurality of consumer records to generate a credit bureau bust out score for each of the subset of the plurality of consumer records; and

store in a storage repository the credit bureau bust out score associated with the subset of the plurality of the consumer records; and

the processor able to run the bust out module.

2. The bust out fraud detecting system of claim **1**, wherein the plurality of consumer records is received in real time.

3. The bust out fraud detection system of claim **1**, wherein the plurality of consumer records relate to prospective consumers that may be approved for credit.

4. The bust out fraud detection system of claim **1**, wherein the plurality of consumer records is received in a batch.

5. The bust out fraud detection system of claim **1**, wherein the plurality of consumer records represent existing consumer accounts.

6. The bust out fraud detection system of claim **1**, wherein the credit bureau bust out model predicts fraud one to three months in advance.

7. A computer implemented method for generating scores that indicate bust out fraud comprising:

identifying a plurality of consumer records;

receiving a bust out filter from a storage repository, the bust out filter created using substantially only credit bureau data;

applying the bust out filter to each of the plurality consumer records to generate a bust out score for each of the plurality of consumer records; and

storing in a storage repository the bust out score associated with each of the consumer records.

8. The computer implemented method of claim **7**, wherein the plurality of consumer records is received in real time.

9. The computer implemented method of claim **7**, wherein the plurality of consumer records related to potential prospective customers that may be approved for credit.

10. The computer implemented method of claim **7**, wherein the plurality of consumer records is received in a batch.

11. The computer implemented method of claim **7**, wherein the plurality of consumer records represents existing consumer accounts.

12. The computer implemented method of claim **7**, wherein the bust out model predicts fraud one to three months in advance.

13. A storage medium having a computer program stored thereon for causing a suitably programmed system to process computer-program code by performing the method of claim **7** when such program is executed on the system.

* * * * *